

REMARKS

Claims 1-9 have been rejected under 35 USC 102(e) as anticipated by Hippelainen. The rejection is respectfully traversed.

The invention is directed to a method for enabling the interception of telecommunication data, where copies of data packets are sent to a monitoring handling device. The handling device forwards the copied data packets data to one of a number of addresses of listening stations (LEA). A monitoring handling device knows the addresses of the listening stations. Hence, data to be intercepted is transmitted to listening stations of different agencies and simplifies key management compared to conventional solutions in which individual connections are from listening stations to interface switching devices. In this case, the transmission of intercepted data is still very secure since an encrypted transmission occurs from the monitoring handling device CIH to the listening stations LEA. AT the same time, it is possible for only one monitoring handling device to be used per public land mobile network or by a number of public land mobile networks.

Hippelainen discloses a method and system for performing a lawful interception in a packet network such as the GPRS or UMTS network. More specifically, a lawful interception gateway (LIG) (similar to a monitoring handling device), initiates the interception of telecommunication data by means of lawful interception nodes (LIN) and forwards received copies of interception data packets to listening.

According to the claimed invention, a monitoring handling device accesses a memory containing a list of keys for listening stations (LEA) and transmits data in encrypted form to a listening station using the key for said listening station. In Hippelainen, there is not disclosure related to information about data encryption. Referring to paragraph [0055] of the reference, this section simply discloses that interfaces X1, X2 and X3 might be used through which the listening stations (LEAs) can be connected to the lawful interception gateway (LIG). There is no disclosure that the X1, X2 and X3 connections are encrypted via keys and saved in the LIG. Hippelainen only discloses explicitly that the data connections between the various LIN and the LIG are encrypted, but in the LIG all encrypted packets are decrypted again.

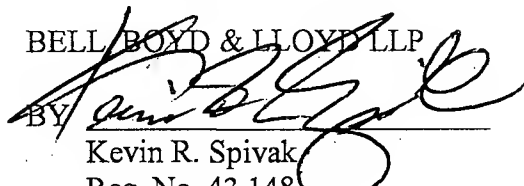
Additionally, claims 1 and 9 have been amended to include that only the monitoring handling stating knows the addresses of the listening stations. That is, only one single central

entity (the monitoring handling device) is capable of communicating with the interception device by means of an encrypted connection and also with the listening stations via an encrypted connection to addresses that are only known to the monitoring handling device.

In view of the above, Applicants submit that this application is in condition for allowance. An indication of the same is solicited. The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing, referencing Attorney Docket No. 118744-128.

Respectfully submitted,

BELL BOYD & LLOYD LLP

BY 
Kevin R. Spivak
Reg. No. 43,148
Customer No. 29177

Dated: October 20, 2008